Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1.   (Currently Amended) A method to manage secure connections, comprising:

receiving ~~an~~ a first initial encrypted packet transmitted from an internal node and addressed to a secure port of an external node;

recording ~~a~~ an unmatched flow comprising an internal address and a security identifier associated with said first initial encrypted packet in a list to designate a secure connection between said internal node and said external node;

receiving a ~~subsequent~~ second initial encrypted packet having a security identifier and an external address that represents a plurality of internal addresses;

translating said external address of said second initial encrypted packet by selecting one of said internal addresses associated with ~~a~~ an oldest or most recently active unmatched flow recorded in said list ~~that comprises a security identifier that matches said security identifier of said subsequent encrypted packet~~; ~~and~~

communicating said second initial encrypted packet to said selected internal address; and

forwarding a subsequent encrypted packet having a security identifier that matches said security identifier of said second initial encrypted packet to said selected internal address.

2

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

2.   (Previously Presented) The method of claim 1, further comprising:

searching a list of security identifiers having associated times;

selecting a security identifier having an earliest time; and

retrieving said internal address associated with said selected security identifier.

3.   (Previously Presented) The method of claim 2, further comprising:

creating said list; and

searching said created list.

4.   (Previously Presented) The method of claim 3, wherein said creating comprises:

receiving an encrypted packet having a predetermined sequence number and a

security identifier from a device associated with one of said internal addresses;

determining a time said encrypted packet was received;

associating said time and said internal address with said security identifier; and

storing said security identifier with said associated time and associated internal

address.

5.   (Original) The method of claim 1, wherein said packet is encrypted in accordance

with the Internet Security Association And Key Management Protocol (ISAKMP).

6.   (Original) The method of claim 1, wherein said encrypted packet is an Internet

Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.

3

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

7.   (Previously Presented) The method of claim 1, wherein said security identifier is a

security parameter index (SPI).

8.   (Previously Presented) The method of claim 1, wherein said security identifier

represents a tunnel between two devices, and further comprising:

receiving a message that said encrypted packet was communicated to an incorrect

internal address;

determining activity levels for each tunnel terminating at each device represented

by said plurality of internal addresses; and

communicating said encrypted packet to an internal address having a tunnel with

a highest activity level.

9.   (Currently Amended) A method to manage secure connections, comprising:

creating a list of unmatched flows comprising security identifiers to designate

secure connections by storing security identifiers in response to receiving initial

encrypted packets addressed to a secure port, with each security identifier representing a

tunnel terminating at a device having an internal address;

translating each of said internal addresses to an external address;

receiving an initial encrypted packet having said external address and a security

identifier;

translating said external address of said initial encrypted packet by selecting one

of said internal addresses associated with an oldest or most recently active unmatched

4

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

flow a security identifier from said list ~~of security identifiers that matches said security~~

~~identifier of said encrypted packet having said external address~~; and

    communicating said <u>initial</u> encrypted packet to said selected internal address<u>; and</u>

    <u>forwarding a subsequent encrypted packet having a security identifier that</u>

<u>matches said security identifier of said initial encrypted packet to said selected internal</u>

<u>address</u>.

10.   (Original) The method of claim 9, wherein said tunnel is created in accordance

with the Internet Security Association And Key Management Protocol (ISAKMP).

11.   (Original) The method of claim 9, wherein said encrypted packet is an Internet

Protocol (IP) Encapsulating Security Payload (ESP) encrypted packet.

12.   (Previously Presented) The method of claim 9, wherein said security identifier is a

security parameter index (SPI).

13.   (Previously Presented) The method of claim 9, further comprising:

    searching said list of security identifiers having associated times;

    selecting a security identifier having an earliest time; and

    retrieving said internal address associated with said selected identifier.

14.   (Previously Presented) The method of claim 9, wherein said creating comprises:

5

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

　　　receiving an encrypted packet having a security identifier from a device

associated with one of said internal addresses;

　　　determining a time said encrypted packet was received;

　　　associating said time and said internal address with said security identifier; and

　　　storing said security identifier with said associated time and internal destination

address.

15.　　(Currently Amended) A secure connection manager, comprising:

　　　a flow module to create a list of <u>unmatched flows comprising</u> security identifiers

to designate secure connections by storing security identifiers in response to receiving

<u>initial</u> encrypted packets addressed to a secure port, with each security identifier

representing a secure flow terminating at a device with an internal address; and

　　　a translation module to select an internal address for an <u>initial</u> encrypted packet

having an external address and a security identifier, said internal address associated with

<u>an oldest or most recently active unmatched flow</u> a~security~identifier from said list of

security~identifiers~that~matches~said~security~identifier~of~said~encrypted~packet~having

said~external~address, and to translate said external address to said internal address for a

subsequent encrypted packet having a security identifier that matches said security

identifier of said initial encrypted packet.

16.　　(Original) The secure connection manager of claim 15, further comprising:

　　　a communication module to communicate said encrypted packet to said selected

internal address.

6

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

17.   (Currently Amended) A system to manage secure connections, comprising:

a first network node to send encrypted packets to an external address;

a second network node to receive said encrypted packets and translate said

external address to an internal address using a list of security identifiers; and

a third network node having said internal address to receive said encrypted

packets,

wherein said second network node receives an a first initial encrypted packet

transmitted from said third network node and addressed to a secure port of said first

network node, said second network node records a an unmatched flow comprising an

internal address and a security identifier associated with said first initial encrypted packet

in said list of security identifiers to designate a secure connection between said third

network node and said first network node, and said second network node translates said

external address by matching a security identifier of a second initial encrypted packet

having a security identifier received from said first network node with a security

identifier associated with a by selecting an internal address associated an oldest or most

recently active unmatched flow recorded in said list, said second network node

communicates said second initial encrypted packet to said selected internal address, and

said second network node forwards a subsequent encrypted packet having a security

identifier that matches said security identifier of said second initial encrypted packet to

said selected internal address .

18.   (Original) The system of claim 17, wherein said second network node is a router

configured to perform natural address translation (NAT).

7

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

19.   (Original) The system of claim 17, wherein said first and third network nodes are

configured to communicate using a tunnel created in accordance with the Internet

Security Association And Key Management Protocol (ISAKMP).

20.   (Original) The system of claim 17, wherein said encrypted packets are Internet

Protocol (IP) Encapsulating Security Payload (ESP) encrypted packets.

21.   (Original) The system of claim 17, wherein said second network node performs

said translation using a list of flow identifiers, with each flow identifier representing a

security parameter index (SPI) and having an associated internal address and receipt time.

22.   (Currently Amended) An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a

processor, result in managing a secure connection by receiving an a first initial encrypted

packet transmitted from an internal node and addressed to a secure port of an external

node, recording a an unmatched flow comprising an internal address and a security

identifier associated with said first initial encrypted packet in a list to designate a secure

connection between said internal node and said external node, receiving a subsequent

second initial encrypted packet having a security identifier and an external address that

represents a plurality of internal addresses, translating said external address of said

second initial encrypted packet by selecting one of said internal addresses associated with

8

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

a~~n~~ an oldest or most recently active unmatched flow recorded in said list ~~that comprises a~~

~~security identifier that matches said security identifier of said subsequent encrypted~~

~~packet, and~~ communicating said second initial encrypted packet to said selected internal

address, and forwarding a subsequent encrypted packet having a security identifier that

matches said security identifier of said second initial encrypted packet to said selected

internal address.

23.   (Previously Presented) The article of claim 22, wherein the stored instructions,

when executed by a processor, further result in selecting one of said internal addresses by

searching a list of security identifiers having associated times, selecting a security

identifier having an earliest time, and retrieving said internal address associated with said

selected security identifier.

24.   (Previously Presented) The article of claim 23, wherein the stored instructions,

when executed by a processor, further result in searching said list of security identifiers

by creating said list, and searching said created list.

25.   (Previously Presented) The article of claim 24, wherein the stored instructions,

when executed by a processor, further result in creating said list by receiving an

encrypted packet having a predetermined sequence number and a security identifier from

a device associated with one of said internal addresses, determining a time said encrypted

packet was received, associating said time and said internal address with said security

9

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

identifier, and storing said security identifier with said associated time and associated

internal address.

26. (Currently Amended) An article comprising:

a storage medium;

said storage medium including stored instructions that, when executed by a

processor, result in managing secure connections by creating a list of <u>unmatched flows</u>

<u>comprising</u> security identifiers to designate secure connections by storing security

identifiers in response to receiving <u>initial</u> encrypted packets addressed to a secure port,

with each security identifier representing a tunnel terminating at a device having an

internal address, translating each of said internal addresses to an external address,

receiving an <u>initial</u> encrypted packet having said external address and a security

identifier, translating said external address <u>of said initial encrypted packet</u> by selecting

one of said internal addresses associated with <u>an oldest or most recently active</u>

<u>unmatched flow</u> ~~a security identifier from said list of security identifiers that matches said~~

~~security identifier of said encrypted packet having said external address~~, and

communicating said <u>initial</u> encrypted packet to said selected internal address, and

<u>forwarding a subsequent encrypted packet having a security identifier that matches said</u>

<u>security identifier of said initial encrypted packet to said selected internal address</u>.

27. (Previously Presented) The article of claim 26, wherein the stored instructions,

when executed by a processor, further result in selecting one of said internal addresses by

searching said list of security identifiers having associated times, selecting a security

10

Appl. No. 10/005,972
Response Dated July 18, 2006
Reply to Final Office Action of May 18, 2006

identifier having an earliest time, and retrieving said internal address associated with said

selected security identifier.

28.   (Previously Presented) The article of claim 26, wherein the stored instructions,

when executed by a processor, further result in creating said list of security identifiers by

receiving an encrypted packet having a security identifier from a device associated with

one of said internal addresses, determining a time said encrypted packet was received,

associating said time and said internal address with said security identifier, and storing

said security identifier with said associated time and internal destination address.